10-9-2008

Resolving the Unexpected in Elections: Election Officials' Options

S. Candice Hoke
Cleveland State University, s.hoke@csuohio.edu

Matt Bishop
University of California - Davis

Mark Graff
Lawrence Livermore National Laboratory

David Jefferson
Lawrence Livermore National Laboratory

Sean Peisert
University of California, Davis and Lawrence Berkeley National Laboratory, peisert@cs.ucdavis.edu

1-1-2008

Resolving the Unexpected in Elections: Election Officials' Options

Candice Hoke
Cleveland State University, shoke@law.csuohio.edu

Matt Bishop
University of California - Davis

Mark Graff

David Jefferson
University of California - Davis

Resolving the Unexpected in Elections:

Election Officials' Options

Matt Bishop, Mark Graff, Candice Hoke, David Jefferson, Sean Peisert[1]

Introduction

Election administrators have had to manage rapid changes in voting equipment, with some shouldering multiple changes in barely three years. Even with ample time, staffing, and technical support, these voting technology changes would present tremendous challenges to the most experienced administrators. The reality, of course, is that optimal resources have not been available to support these relatively quick changes in core equipment.

The record is clear that rapid changes in major election equipment, and consequently in the operational procedures, protocols, and ancillary equipment carefully designed to support those systems, can disrupt the best administration and place great stress on already overburdened staff. Add in the presidential election cycle's high volume of voters and new voter registrations, plus intense public and media scrutiny, and the situation can move from bad to worse. Small mistakes are magnified and can lead to unfair accusations of poor planning or political favoritism. Topping off the situation, the computer-based voting systems that were touted as problem-solvers have in some instances become the source of new challenges, frustrations, and anxieties.

---

[1] The authors have expertise in computer science and engineering, computer forensics, voting technology evaluations, and election administrative processes; detailed background information can be found on pages 19-20. Author affiliations are provided for identification purposes only: Matt Bishop (University of California at Davis); Mark Graff (Lawrence Livermore National Laboratory); Candice Hoke (Cleveland State University); David Jefferson (Lawrence Livermore National Laboratory); Sean Peisert (University of California at Davis).

This paper recognizes the reality of election administration going into a major presidential election. It does not rehash the merits of e-voting or the debates over which type of voting equipment is better than others. Nor does it criticize the equipment undergoing final preparations for use in the November 2008 general election. All of these voting systems have plusses and minuses. Like most other computer-based equipment, these systems can be expected to perform relatively well for their intended tasks. But computer-based voting equipment also presents possibilities of some unexpected, technically odd behavior that can disrupt election preparations, balloting, or tabulation, and can lead to inaccurate results. A quick managerial review can often identify the cause of the problem, and lead to a simple and complete solution, especially where the technology is familiar. But election officials have advised us that at other times they could not determine the cause and thus left it uncorrected, hoping the election would run smoothly and totals would reconcile.

This paper is designed to assist election officials in effectively handling the technical irritations that have been difficult to diagnose, allowing them to protect themselves and the public interest from unfair accusations, inaccuracies in results, and conspiracy theories. The paper's primary goal is to empower officials to recognize which types of voting system events and indicators need a more structured analysis. Its approach seeks to enable officials to evaluate what the next steps should be, and to help them prepare for an inquiry should they decide to schedule it. The authors emphasize that ***computers can produce incorrect results***, because of programming errors, incorrect settings, or insufficient built-in safeguards. ***No deliberate wrongdoing need occur for computerized voting equipment to fail to perform correctly and no "operator error" need occur***—but these are points some fail to grasp when they lodge accusations rather than wait for the truth to come out.

An objective, arm's-length examination conducted according to professional standards of allied fields (primarily computer forensics) can:

- determine both causes and solutions for unexpected and unexplained technical issues;
- settle questions and lead to broad acceptance of the ultimate report of election results, despite serious questions triggered by a technical equipment performance problem;
- reduce or eliminate the need for a complete hand-count of affected ballots;
- stop wild speculations and the "rumor mill";
- reduce election litigation; and
- enhance the public's confidence in the election officials entrusted to conduct the elections and reduce reputation injuries fueled by lack of objective information.

Depending on the evidence made available, the quality of the team, and the scope authorized for the review, election officials can obtain the information needed to resolve the problem, determine and validate election results, activate warranty repairs, and—in many cases—learn how to prevent a recurrence. Others involved in resolving questions about election processes and results, such as election agency lawyers, candidates and political parties (and their lawyers), initiative sponsors, advocates, consultants, vendors, and policy makers, may also find this paper useful.

I. The Problem

During an election, an optical scanner may fail to read ballots consistently, or a server may freeze as it tabulates votes. Perhaps voting machine memory cards or optical scan ballots appear to be missing in the canvass report. Every election cycle, experienced election administrators around the nation anticipate and successfully cope with events like these. But sometimes initial and secondary troubleshooting steps don't work. Election results totals cannot be reconciled, for example, or seemingly inexplicable equipment or software failures recur. The vendor's manuals do not provide sufficient direction to correct the situation. Facing election reporting deadlines and legal duties to report accurate totals, election officials need answers. What happened? Are totals accurate and complete? Can they in good conscience certify the results of this election before the answers are found? Delays and unusual computer events can also raise questions from others. Candidates might want to know whether the problem affects their race, and whether the problem is serious enough for them to request a recount or other remedy.

The technical explanations needed to answer such questions are in the realm of ***election forensics***: the process of analyzing and discovering the causes and cures of odd technical occurrences that occur in elections and might have had an impact on the validity of the results. Since the problems involve computers, as they often now do, then ***computer forensics***—the specialized procedures, tools, and skills needed to diagnose complex hardware and software problems are likely a large part of the expertise required. Unlike the television presentation of forensics, the forensics field is not primarily criminal. Forensics specialists are, however, dedicated and expert mystery-solvers. Computer forensics specialists are trained to solve technical puzzles that require that they handle the software, hardware, and other materials in a manner that is legally approved—which is a similar context to that of election officials.

The forensic specialists can be asked to determine: what caused the unexpected computer behavior? Were the vote totals affected? Can the voting records be recovered? How can we prove the voting data was not injured, to public satisfaction? Even jurisdictions that use voter-verified paper ballots will find that this form of balloting is often not enough to answer oddities that will need to be resolved, for instance, to explain a discrepancy between electronic (computer-produced) and paper ballot vote counts.

The authors of this paper recognize that few election offices are sufficiently large and well-resourced to have on staff or by contract an independent computer security or forensic specialist. Thus we have written this paper, drawing on the fields of election technology, computer forensics, and computer security, so that all election administrators and their counsel can consider when additional election troubleshooting and forensic steps should be taken. In this paper, we do our best to answer the following questions:

- When should election administrators consider an election forensic examination?
- What questions can the examination answer?
- How should they prepare for an examination?
- Who should be included on the forensic team?
- What sort of contractual provisions may be needed?

Thus, this document provides an introductory overview to election forensics rather than an instruction manual for a forensic examination.

II. Indicators for a Forensic Examination

Dozens of technical problems, major and minor, can occur during an election. The specific problems will depend on the particular voting technology used in the jurisdiction, the vendor, the software version and configuration, and the kind of election involved (general, primary, special, recall, plurality, instant runoff/rank choice, etc.). The vast majority of technical problems are simple, recognizable, and fairly routine, and can be resolved by standard procedures such as rebooting; replacing or recalibrating a piece of hardware; applying documented workarounds for known problems; or by conducting cross-checks, pre-election tests, and post-election auditing processes. Such routine problems are familiar to election officials everywhere and clearly should not trigger any formal examination.

Occasionally, however, an event occurs that is outside the normal range of familiar problems. A system may crash, or yield inconsistent preliminary election results in one or more races. It may simply behave in an unexpected way not previously seen or documented (sometimes called an "anomaly"), and perhaps not repeatable. Perhaps surprisingly, the very non-repeatability of a problem may itself be a key indicator that something more fundamental is wrong. Such unusual or unexpected events could result from a hardware failure, a ballot definition error, an operator or poll worker error, a previously unknown software limitation or bug, or a combination of such causes. Also, the possibility of election tampering through either malicious software or direct human alteration of vote totals cannot be casually dismissed, though we will only briefly discuss it here.

A note on terminology: a problem should never be summarily described as a "glitch," "hiccup," or "computer error." Such terms, and other similarly dismissive, pseudo-technical words and phrases, are inappropriate in serious contexts and thus should be eliminated from discussions of elections technical irregularities. These words tend to minimize the significance of unusual or unexpected events by suggesting that computer behavior is somehow inherently unpredictable, that no human error could have been involved and thus the incident is not worth inquiry or remedy. On extremely rare occasions, a problem may indeed be caused by a transient, random hardware failure, but those are far more rare than most people believe. It is safe to say that when a problem occurs, some human error is involved, usually by a system architect, a vendor software programmer, a technical support contractor, an election official, or an IT staff member.

Whenever a technical issue surfaces with voting equipment, election officials should undertake an inquiry as to its causes and cures. Even if a problem ***seems*** small and inconsequential, that does not necessarily mean the problem is trivial and needs no examination. Like the proverbial tip of the iceberg, small problems may be the only observable signs of large or systemic underlying problems. Even if the outcome of a particular race does not appear to depend on resolving the problem, conscientious election officials should examine it. This inquiry helps both the jurisdiction where the irregularity surfaced as well as other jurisdictions, for often, like icebergs, the underlying problem is present elsewhere but without visible symptoms or indicators—which might mean the problem goes undetected when it most matters. All unusual or unexpected events in voting systems, as in any high reliability, high security computerized systems, should be examined. One option to consider is a forensic examination of the computerized voting system components related to or potentially affected by the problem.

Examples of the kinds of unusual or unexpected events that should be cause for considering a forensic examination are set out below. All of these events have occurred at one time or another

in the last few years in at least one U.S. election. This list, however, should be considered as illustrative, and by no means exhaustive. Any unusual or unexpected behavior, even if not on this list, should trigger consideration of a forensic examination.

A. General problems with electronic voting equipment, such as:

- Repeated "crashes," "freezes," or auto-reboots of any voting system component
- Components that become slower and slower the longer they are in service
- Unusual episodes of unresponsiveness that last more than a few seconds
- Failure of some usually reliable functionality
- Unusual or undocumented error messages from the application software of any component
- Unexplained and undocumented new system behavior, even if it occurs only once
- Failure of a post-election logic and accuracy (L&A) test of any component (especially if the same component passed its pre-election L&A test).

B. Issues with election results, vote totals, or other data:

- Any unresolvable failure of vote totals, ballot counts, or voter counts to properly sum and reconcile with each other, or with audit trail records
- Unusually high numbers of overvotes, top of ticket undervotes, write-in votes, or votes for minor candidates or parties
- Vote totals that are obviously too small (or negative), or obviously too large, even if they appear to reconcile properly
- Any inexplicable or illogical data (or indicators of data corruption), including in vote totals, database time stamps, or automatic audit logs.

C. Specific issues with electronic equipment:

- Memory cards or cartridges that, when read repeatedly, appear to give different results, or read errors
- Memory cards or cartridges that are supposed to be redundant copies of one another, but do not in fact contain identical data
- For direct recording electronic (DRE) systems, any discrepancy at all between the results reported electronically for a precinct and the results of a hand count of intact voter-verified paper audit trail (VVPAT) records for that same precinct
- For DREs, multiple reinforcing reports of failure of the votes as recorded on the summary screen to agree with the voter's tentative votes or with the VVPAT
- For optical scanners, any batch of paper ballots that, when read repeatedly by the same or different scanners, yields counts that differ
- For optical scanners, any failure to scan and properly record the votes of a test deck that contains clean, correct marks.

D. Problems reported from the field:

- Multiple corroborating reports from voters, poll workers, or county employees that the

voting equipment is not functioning properly (regardless of whether they explain the problem correctly.

Regardless of whether they appear on this list, any technical events or data records that cannot be explained and resolved are candidates for a forensic examination.

III. Questions a Forensic Examination Can Address

It is important that the members of the forensic team work with election officials to determine the questions and parameters for the examination. The questions that the public may have most in mind for the forensic examination to answer are: *Was the election called correctly?* Or, *Can we correctly announce the winners now?* Answers to these questions, however, generally extend beyond the technical issues the team is qualified to address. The examination will provide insight into what caused the problem, how to recover voting data if necessary, and whether there are technical issues that would throw the results of the election into doubt. Election officials can then use this information in fulfilling their duties to certify accurate elections, and take care of valuable election equipment.

A. Some Appropriate Questions

The following are examples of technical questions that the forensic team may well be able to answer. Obviously such questions should *guide* the examination, and not *limit* it.

- How many votes did the problem affect (minimum, maximum, best guess)? How accurate are the (preliminary) canvass totals?
- If the totals are wrong, can you recover the data (votes) needed to correct the totals?
- Is the computerized voting equipment operating in accordance with its documentation?
- Were any procedural guidelines violated that might have contributed to the cause of the problem?
- Does the problem affect only this jurisdiction, or might other jurisdictions have the same problem?
- Did you find anything that appears, in your judgment, to be evidence of negligence, malfeasance, misuse, or attack?
- What can or should be done to prevent the problem from recurring, short term (in the way of procedural workarounds) and longer term (in the way of software or hardware changes)?

Officials might ask the team additional questions to obtain more detailed information, including whether the examination discovered anything that might indicate a significant malfunction of the computer hardware or software, a deliberate attempt (failed or successful) to affect the vote statistics or to interfere with voting, or serious errors in instruction manuals or documentation.

B. Some Inappropriate Questions

Good team members will restrict their focus to providing technical information, recommendations, and conclusions. Other questions lie beyond the elections forensic team's expertise and they will not be able to answer:

- Should we get rid of these machines or buy more of these machines? (A business judgment decision.)

- Should we sue someone? (Asks for both a legal opinion *and* a business judgment decision.)

IV. Preserving Forensic Evidence

If election officials decide that a forensic examination is a prudent next step, they should take preparatory measures to increase the chances of success and reduce the possibility of procedural, technical, and legal errors. Later in this paper, we address a third area of preparation: laying legal and contractual foundations for the work.

Forensic examiners gather evidence and analyze it to determine the nature, cause, and effects of technical problems. To make that possible, election officials must preserve the relevant evidence. Since examiners will not initially know what evidence they need and almost anything could be important, ***everything that might be relevant should be preserved***. Where circumstances prevent freezing or capturing the evidence, for instance, an error message, a digital photograph can assist in documenting events and contexts for later use.

All forensic examinations (election-related or otherwise) are based on the principle that the ***evidence must be preserved in a credible manner***. The forensic examiners' tasks require that they interpret the evidence to determine what happened in a way that others can validate. If the evidence is not preserved during the examination, the forensic findings are immediately suspect. Further, in a situation as volatile as an election, observers may want (or need) to validate the examiners' conclusions. If the examiners cannot show the evidence has been preserved, others cannot perform this validation, raising questions about the examination's results. In general, evidence handling should be minimized and the chain of custody should be tracked regardless of whether that evidence is on paper, data disks, software, logs, machines, networks, or something else electronic. This means that election officials need to have a process in place for documenting how to handle potential evidence. The process the jurisdiction normally uses to track paper ballots may be sufficient.

The credibility of the forensic examination is paramount, and must be achieved in two separate ways: first, credibility of the preservation of evidence; and second, openness of the examination. If people do not believe the evidence has been preserved, they will question the validity of the examination's conclusions. Here, the "chain of custody" records figure prominently. In addition, it is strongly recommended that ***no one ever be left alone with potential evidence*** including chain of custody records. This ***"two-person rule"*** means that at least two people can vouch for the accuracy of the chain of custody records. This rule applies to original evidence; of course, one person can handle copies of evidence alone.

Second, if an examination is conducted in secret, often the public response is to doubt its results, regardless of how well the evidence was preserved. Given that elections in the United States are traditionally conducted openly, with a minimum of secrecy (for example, in some States, observers can view every step of the process except the voter casting her votes in the booth). This expectation of openness naturally extends to examinations of equipment issues that could affect election results. Thus, the public should be able to observe all activities before and during the

examination. Of course, this openness needs to be balanced with the need to maintain the confidentiality of examiners' discussions as they are conducting the review, and to protect the vendors' proprietary information. For example, the California Top-to-Bottom Review [1,2] used cameras to broadcast video to a public area apart from the secured facility where the "red team" analysis was conducted. Audio was not provided, however. Any member of the public could thus come to watch the examination—and the examiners could speak freely about confidential information and their testing and preliminary conclusions, without premature disclosures.

A. Preserving Paper Records

All paper records relating to registration, voter sign-in at precincts, VVPAT records, and ballots must be preserved as required by law, of course, including spoiled ballots, provisional ballots, absentee ballots, and unused ballots, signed "zero tapes," end-of-day precinct tally sheets, and signed poll worker records. The examiners may need to re-reconcile the precinct voting data.

1. A wide array of ***installation, inventory,*** and ***repair records*** is important, including those of:

- firmware and software versions
- hardware installations
- L & A (logic and accuracy) testing
- machine malfunctions, crashes, failures, and other prior unusual or unexpected behavior
- software patches installation
- workaround programs.

If the records are not available, forensic examiners may also have to create a list of all files and software, including version numbers and dates of installation and last modification.

2. Precinct and voting records that might be needed include:

- serial numbers of the machines and memory cards that went to each precinct
- which memory cards were used in each machine
- precinct or early voting registries.

3. Records of individuals' access to the relevant machines and security equipment are equally important. These records should detail:

- names of people who had access to voting machines, and at what times and locations, including voting system vendor employees, poll workers, technical services contractors, transport and delivery personnel, and others who had custody of various pieces of system equipment
- security video tapes
- chain of custody records for the voting machines, memory cards, paper ballots, and other election materials
- the numbers or codes of tamper-evident seals.

B. Preserving Machines

A general rule is to ***preserve equipment when the problem is discovered***. This section describes what to save. But in practice, if the problem occurs during the election, the equipment often must continue to be used because the election cannot be stopped. In that case, copies of the data on the equipment—for example, making backups—will preserve much of the information for the examiners. Digital photographic records can also prove helpful.

For an electronic forensic examination, ***all voting system equipment***, including the precinct devices (e-voting machines, printers, monitors, registration check-in devices, etc.) as well as county-level devices (card readers, ballot counting devices, servers) should be preserved until the examiners and officials determine the scope of the review. Further, if a computer or device involved in the election is running at the time the problem was discovered, it is best for the examination if it is left running so that, for example, it is possible to determine what software was running when the problem was discovered. If the device or computer was off when the problem appeared, it should be left off.

If the machines are connected to a network, forensic experts will decide what to connect or disconnect from the network. The network containing machines involved in the election should not be altered. It should be left as it was when the problem was discovered. If this is not possible because, for example, the machines are at a polling station, officials should keep detailed records of what staff did and any events that occurred after the problem was discovered. The physical environment in which the equipment was located should be left undisturbed or, if that is not possible, photographs and measurements should be taken.

Additional equipment to preserve includes:

- ***Memory cards and sticks***, which are critical components for review, so special care should be taken to inventory and account for them. They are central to the security of the systems and also typically contain automatic audit logs crucial to any examination. Any memory devices should be left where they are. Other memory cards that are not in use should be preserved and definitely not inserted into any machine. Under no circumstances should any memory card be modified or erased except by the forensic examiners, and governing law may prevent any changes in recorded memory.
- ***All redundant memory*** in the machines (as data in e-voting systems is generally stored on multiple "independent" memory devices, all must be preserved). These vote records that were generated "closest" to the voters are a top priority.
- ***Poll closing tapes*** (e.g., from VVPAT printers, scanners, ballot marking devices).
- ***File systems and files on all relevant machines and devices***.

Once it is clear a forensic inquiry will be convened, no one other than forensic examiners should touch any of the equipment or files. Everything connected with the election should be frozen and maintained as close as possible to the state it was in when the problem was discovered. Preserving the environment and materials extends to the computer environment. No personnel should create, open, edit, or delete files, run programs, log in or log out.

V. Providing a Facility

Depending on the scope of the forensic examination, the team may require a secure area in which to work, i.e., a physical facility with controlled access, such as a conference room or some office space that can be locked and has alarms. The members of the forensic team should generally be able to control who is allowed to access that space. It should be large enough to house:

- Paper and other physical evidence
- The computers involved in the examination; the team can determine whether all computers need to be housed in the space concurrently
- Any other equipment relevant to the examination or that the team needs (for example, cameras, recorders, printers, laptops, etc.)
- The people on the team, as well as any other authorized personnel such as observers.

The team will probably also want an office safe to lock sensitive material such as notes, disks, and laptops when their protocol requires it, or when no one is present. Past examinations have found something on the order of eight cubic feet of locked space to be adequate.

Within the secured space, the team will need access to the Internet for sending and receiving email and for conducting Web searches (which can be helpful when conducting forensic analysis). Under *no* circumstances will they connect any voting system component to the Internet. (No voting system component should *ever* be connected to the Internet, even during forensic examination.) Depending on the type of problem, the forensic team may, however, need to connect the voting system components to one another or to their own computers for diagnostics, which will require one or more internal networks within the secured space. The best way to guarantee network security in the secured space is by keeping all other networks physically separated from the one connected to the Internet.

VI. Composition of the Forensic Team

As described in the Introduction above, most technical problems that arise in elections are routine, and are handled without difficulty by election officials and their IT staffs. However, when an unusual, unfamiliar, or confusing event or result occurs, then much broader and deeper technical expertise is required to diagnose and resolve the problem than most counties or Secretaries of State have on staff. That expertise is the key asset that a forensic team brings to the table.

A. Team Organization and Size

Depending on how many different types of devices or how much software is involved, some inquiries may need more people, more time, or consultation with other experts. Many technical issues, perhaps most, are caused at least in part by the failure to follow some procedural requirement for setting up and using the computer-based equipment. Thus, except when unusually complex events occur, a team of two to four people will usually suffice but they all must bring special expertise to the project. Occasionally only one well-versed individual has been contractually brought in for a forensics review—a computer science/voting systems professor who was supported by graduate students. Normally, team members will be a group of individuals

recruited by a project leader appointed to head the inquiry [1,3,5,6,7], or from a single firm [4] contracted for the purpose of the forensic inquiry.

B. Technical Qualifications

A good team brings a special set of talents and skills that are unusual even among experienced programmers. Team members will need to learn their way around a complex system that not only did they not help build, but may have never previously seen, all in a very limited time. They will have to quickly discern the design principles and conventions used in building the software and hardware, and its likely strengths and weaknesses. There is always the possibility that a deliberate attack caused the problem—after all, business, educational, and other governmental computers have been attacked, so why not election systems—and only an expert will have the knowledge, skills, and tools to be able to determine what happened in those cases.

All types and components of electronic voting systems, including optical scanners, DREs, automated ballot marking devices, and their election management software are complex computer systems. They use a wide variety of technologies such as memory, operating systems, applications software, programming tools, databases, and security and cryptography. Obtaining a correct architectural and operational understanding of how they work together is the grounding for the forensic examination. The nature of these software programs greatly complicates a team's quick grasp because these large programs are usually written in pieces, at different times, by different people, in different programming languages, and use specialized technologies.

To obtain this system comprehension, the team must have the capacity to read and analyze the systems' source code, and from that determine the functionality of the system. At least one—preferably two—team members must be experts in computer security and forensic analysis. It is not necessary, or sufficient, for the team members to be "certified" by various companies or institutes such as CISSP, GIAC, or SANS. But the team must know, or be able to learn quickly, how to set up the systems in question, and how they could be set up in other ways (this will help them uncover problems arising from not following recommended set-up procedures); how to recover deleted files; and how to make copies of the systems' memories and disks without disturbing the contents of the original memory and disks in any way. As an example, for Windows-based election management systems and canvass servers, the team will need to access the multiplicity of logs that Windows keeps. Another example: the team may have to set up tests to analyze the voting system software and observe it execute in order to test possible causes of the problem. This would be done on copies of the systems, not on the actual systems. A good forensic team can perform these tasks.

To conduct these analyses, then, at least one team member must have knowledge of the architecture of one or more voting systems. Individuals who have participated in reviews of these systems, or who have studied reports describing the architecture, source code, operations, and vulnerabilities of deployed voting systems, or who have co-authored these reports, will provide significant insights into the use and examination of these systems. They will be able to use their experience and knowledge to diagnose problems and identify solutions more quickly than examiners without this experience and knowledge. But other computer scientists, software engineers, or computer security and forensics firms could get up to speed by studying the published voting systems studies (see Appendix 2).

Finally, at least one team member must have expertise in election administration and procedures. Election management is a legally intensive and unusually complex set of time-bound interconnecting processes that must sequence almost perfectly for the election to be conducted successfully. As officials know, ballots and voting machines must be properly configured, tested, and delivered on time, with poll workers properly trained, voting locations open on time, tabulation equipment functioning properly, and all memory media and voting data returned promptly—and each of these tasks requires a myriad of subtasks to complete in sequence. Normally, an election forensic examination is also under severe time pressures, and there will be little time to explain and bring team members up to speed in the nuances involved in election administration. With a team member well versed on these essential administrative points, the review can be conducted far more quickly.

C. Non-Technical Qualifications

As with examiners or auditors in any other field, at least three qualities are essential: objectivity, the freedom and willingness to follow the inquiry wherever it goes, and the ability to describe the causes of the problem completely and accurately without regard to potential organizational embarrassment. In sum, the forensic team must have ***independence***.

Strong ethics are essential: the forensic team members must have ***no conflicts of interest, nor the appearance of conflicts*** of interest. If at all possible, they should be entirely disinterested in the results of the election being examined. If that is not possible, the forensic examiners must be able to set aside their interests and undertake the examination without bias. Otherwise, the results will not receive the trust and legitimacy needed by all parties, including the public.

The need for independence and avoidance of conflicts of interest leads to the necessity of not including on the forensic team governmental IT employees (county or State), nor representatives from the voting system vendor. The county or election office IT personnel who helped run the election and the vendor technical representatives who know the systems intimately, are crucial ***resources*** for the forensic team, but their role must be limited to providing information to the independent forensic team. This role is discussed in more detail below.

Finally, the team members must be persons of high integrity and good judgment, and must not be associated with any partisan organization involved in the election. There may be a great deal at stake in the resolution of an election problem. The outcome of important races may hinge on the results of the inquiry. The problem may have besmirched the reputations of election officials, the vendor, and other participants. The problem may have shaken the public's confidence in the election. The members of the team must have the temperament to be rational, fair, and restrained in their demeanor when writing and speaking about the examination. They need to be able to put aside any opinions in order to find the truth in the inquiry, whichever way it cuts.

D. The Role of the Vendor

Cooperation of the election systems vendor is critical to the examination's success and credibility. The vendor can promote a positive public perception of its company despite the technical problem if it fulfills its unique role as a resource and support for the team. Under no circumstances should an election jurisdiction forego a forensic analysis of a problematic election because the voting equipment vendor opposed it or suggested an explanation for the problem.

Nor should the vendor apply pressure on a jurisdiction to accept its explanation and bypass having its hypothesis independently confirmed.

Though the vendor is critical to the success of the forensic review, the public agency must not allow the equipment vendor to appoint any examination team members. The basic rule is: ***the vendor must be a resource for the team, but must not conduct or participate in conducting the examination.*** Three important reasons lead to this conclusion.

First, forensics team members must approach the examination with ***no preliminary conclusions of what caused the problem***. In practice, this means they must be prepared to follow the evidence. An examiner who has a "pretty good idea" of what happened, and why, before the investigation begins may be predisposed to overlook and misinterpret data. The vendor representatives are likely to have less than an open mind to the range of possible causes and solutions. But a vendor can and should communicate its hypotheses to the team, so the team can determine how and to what degree they should explore these ideas.

Second, voting equipment vendors have a direct conflict of interest. Certain types of diagnoses and conclusions will not assist the financial interests of the vendor. Thus, the *human* and business tendency is to try to identify some explanation other than, or in addition to, equipment problems. In some cases, the equipment will be blameless, but in others some aspect of the vendor's activities—perhaps in programming, or in supplying correct documentation—it will have played a major role in the technical disruption. ***The examination should not be biased either way***. If a vendor conducts the examination, a significant portion of the voting public will not respect the examination's conclusion despite ample supporting evidence simply because of the financial conflict of interest. The presence of this conflict taints the integrity of both the examination and the people who selected the examiners. Best choice? Avoid the problem by authorizing an arm's-length examination.

Third, the vendor plays a critical role as an ***information resource***. The examiners will need to learn exactly how the specific equipment is set up, how it is operated, and how the software works. Often, a day spent talking with the vendor personnel can give the team insights that will speed the investigation greatly. We emphasize that ***the purpose of this vendor communication is to guide the examiners' understanding of the system and its use,*** and only that. The vendor should endeavor to fulfill this vital role that it uniquely holds.

The team's communication with the vendor must be handled carefully, to preserve the public perception of the integrity of the examination, as well as its actual integrity. The team must be free to communicate with the vendor for technical information, but if at all possible the convener-sponsor of the examination should also be present. If the vendor wishes to communicate with the team, it should do so through the sponsor and not contact the team directly. This arm's-length relationship may seem extreme, but it prevents the vendor from applying any pressure on the examiners and further promotes the review's integrity.

The vendor must be allowed to respond to the forensic examination team's report. The ***vendor response must be separate*** from the examiners' report, to emphasize the independence of the investigation. Whether the vendor's response is to be made after the examiners' report is publicly issued (as was done in the California Top-to-Bottom Review [3]), or whether it is to be given to the examiners before their draft is made public so the team can take the vendor's comments into account (as was done with the RABA review [4]), is something to be decided and recorded contractually. The advantage of the former is that the public will understand the vendor played

little to no role in the investigation; the advantage to the latter is that potential factual mistakes (such as from second hand information) can be identified and more fully researched so the final report is completely accurate. As long as the ***team's independence and integrity is not simply assured, but also perceived as assured***, either method works.

The vendor is a critical and key resource for the examination, and must be engaged to provide the examiners with technical and procedural information about the equipment and how it should be used. ***If the vendor promptly and completely supports the examination, the vendor will be and will be seen to be an asset to the examination***. It can credibly present itself as a company that is concerned about the quality of its products, their correct use, and the larger public trust embedded in the elections process.

VII. Legal, Contractual and Practical Issues

A. Overview

Given the great importance voters place on the integrity of their election processes, election officials who take an immediate, vigorous public stance detailing what steps will be taken to examine the technical irregularity and its impact will be the best assurance to the public that their interests are being fully protected. Yet before forensic examiners can begin work, contractual and legal issues must be resolved. If the outcome of an election hangs in the balance, even a one-week delay can be too long. To avoid this time loss, the best plan is to prepare in advance a sample set of fair and responsible contractual terms for the forensic inquiry. The contractual issues are generally similar whether the forensic team is from a private firm or is a team of independent scientific experts, or whether county election officials, a Secretary of State, a court, or some other authority has retained the examiners. We must note that this discussion is simply to provide an overview of some contractual and legal issues that will arise and ***not to provide legal advice*** or an exhaustive review of all the law that may govern or the legal issues that could arise; legal counsel should be sought. [7.1] Its length derives from a desire to help others avoid the weeks of difficult contractual negotiations that have delayed some previous examinations.

B. Preparation and Stakeholders

In a small local election, county election officials may be the sole decision-makers of whether to convene a forensic inquiry. In federal elections, such as the presidential cycle, the decision over what type of inquiry and what team credentials will be required will often involve national political parties, presidential candidates, the Secretary of State (or other chief State election officer) along with the State Attorney General and county attorneys, all negotiating a process for forensic review. This wide involvement owes in part to the legal fact that our elections are conducted under an interwoven fabric of Federal and State law and are intensely political processes.

The importance of elections and their relation to control over the levers of power can lead to the remote possibility that prosecutors of either (or both) Federal or State/county government will intercede where unusual technical events occur and block an examination convened by the local officials. The increasing frequency of documented unexpected technical events, however, actually tends to reduce the likelihood of prosecutors becoming centrally involved, an ironic silver lining for public transparency. When prosecutors move in and assume investigatory control, closing out public access and transparency, the rumor mill and conspiracy theories often take over. Public

confidence in the integrity of the election and its administrators can plummet even if later the officials are exonerated.

Fortunately, most prosecutors have sufficient experience with computers and computer forensics to know that computers are far from infallible and that technical irregularities during elections are far more likely to occur for reasons such as programming errors rather than deliberate cyber attack or criminal conduct somewhere within the election administrative system. Knowing the public's inferences—of presuming criminal conduct when formal prosecutorial investigations commence—prosecutors may rather choose to seek involvement in helping to structure an independent forensic examination whose report will also come to their office as well as to the election officials and public. Further, they may seek an informal or formal agreement concerning the handling of evidence (ensuring that if evidence suggesting deliberate wrongdoing is discovered, it will be preserved in a legally sound manner), and the duties of examiners to report potential wrongdoing.

Regardless which stakeholders seek to play a role in determining the scope and composition of a forensic inquiry, election officials will want to ensure that they are fulfilling all obligations imposed on them by law, including any fiduciary duties for assuring an accurate election.

C. Timeline, Authority, Scope, and Public Relations

Timeline: In most election forensics examinations, the resource in shortest supply will be ***time***—especially if the outcome of a race is in question. Forensic examinations almost always take several weeks; particularly difficult ones may take two months. It is essential to plan to devote the time (and funds) needed for a quality review. A good forensic team may decline the job if the schedule is too compressed for the job to be done properly. If the outcome of a race is in question, a target date should be set in the contract for completing the examination, with some flexibility for adjustments. If no race results are drawn into question, it may be possible to have a more open-ended examination in which the timeline remains flexible according to what is found.

Authority: Election officials possess legal authority over the election equipment and materials. But a prosecutor, court, or legislative inquiry might displace their role. It is understandable that government officials will want to be involved and remain informed throughout the process since they have the ultimate responsibility for the proper conduct of the election. But the forensic team needs freedom to act within its charge according to its own direction and schedule. It also needs to be able to ask questions of anyone who might be able to provide information, including election officials, vendor employees, poll workers, and even voters. These access points for relevant evidence need to be stated contractually.

Scope: All parties will need to agree on the goals and parameters of the examination—what they can and cannot do. That way, all parties are likely to understand their tasks and responsibilities. Experience has shown that examinations have difficulties when these parameters and goals are not agreed to before the team begins its work. But the scope of a legitimate forensic examination has to be very wide and open-ended. If a forensic examination is called for at all, the problem by definition defied easy explanations and diagnoses. The examiners must not be limited, for example, to examining the hardware or software of just one component of the system, nor can any component be excluded from examination; once the review is underway, however, and initial diagnostics are complete, reviewers can often narrow the scope and not need to review all components.

Within reason, the team needs the authority to go wherever the examination leads. In the course of their examination, the examiners may come across potential problems in the voting system that in the end are not related to the problem that prompted the examination but which had to be pursued until they could be eliminated as a contributing cause. While the forensic team should generally stay within the scope originally assigned, the contract should specify that they must report significant flaws or vulnerabilities they happen to discover in the course of their work whether within the scope definition or not. The scope's limitations can also be stated, such as if evidence of malicious code or other attacks is found, the team is to refer the matter to the jurisdiction's legal team or the prosecutor.

Public relations: The public has a legitimate strong interest in election accuracy and thus in obtaining knowledge of the outcome of forensic examinations. For efficient and accurate communications, the contract will specify a single point for communication on both the examination team and the convening government entity to which the team will report. An update frequency might be specified, including whether the team spokesperson will be expected to communicate directly with the public via media events after the report has been submitted. This agreement should balance the need of the examiners for freedom from interference, and the needs of the candidates, the vendor, and the public to follow the examination's progress and learn its results.

D. Indemnity, Nondisclosure, Statutory Barriers, and More

Indemnification and Costs of Defense: A settled part of most States' law is indemnification of agents for reasonable costs incurred that are attributable to the agreed work. Like other agents, the forensic examiners will expect to be shielded from any lawsuits that might result from their work, provided their reports are not slanderous and they obey the other contractual clauses. Quite often, this protection can be provided easily by explicitly stating that the forensic examiners are acting as agents of the county or State government [3] that conducted the election and that costs of defense will be assumed by the government entity. Under some State procedures, the forensic examiners may be protected as agents of a court that orders the forensic examination. The lawyers for the election jurisdiction that retains the team will need to research and provide fair indemnification and cost of defense terms, for without it the effort to recruit qualified professionals can be severely impeded.

Nondisclosure Agreements (NDAs): Often, a voting system vendor and the government agencies that procured the equipment have agreed to be covered by a nondisclosure agreement. Leaving aside the question of whether there should be NDAs for voting system technology, such terms are a part of some procurement contracts. It may be necessary that these NDAs be extended to cover the forensic examiners. The forensic team or their firm will usually be willing to sign a narrowly drawn, limited NDA to protect the intellectual property of the vendor that is not within the public domain. (Appendix 1 provides an example.) But most experienced forensic teams will refuse to sign any broadly worded, unbounded NDA since it may expose them to unnecessary liability and could impede the forensic examination report and conclusions from becoming public. If, as has occasionally occurred, a vendor objects to anyone other than the government employees of the election jurisdiction conducting the examination and claims that an existing NDA bars such access for retained experts, the contractual classification of the team members as the jurisdiction's "agents" is often enough to eliminate any difference in access between the team and employees. In the next generation of voting equipment procurements, purchasers would be wise to include provisions specifically authorizing forensic examinations and the NDA terms, if any, when officials

choose to convene an inquiry.

Confidentiality and publication: The public has a strong interest in the publication of a detailed report on the team's findings. The only information that normally should be withheld in the published forensic examination report is information that is either: (a) legitimately proprietary to the vendor and not in the public domain or available beyond the vendor's personnel, or (b) concerns specific details of security vulnerabilities that might be exploitable in an election in the near future, before the problem can be corrected. The exploitable details of security vulnerabilities should be written up in a separate report that is not made public but the recipients and protections for this confidential report should be described in the contract. The scope of "proprietary information" should be defined so that it cannot be interpreted to bar from public access the forensic examination's general findings. One approach would be to incorporate by reference the "industry standard" of disclosure that the California, Florida, and Ohio Secretaries of State and vendors agreed to in the reports under those offices' sponsorship. An additional clause to promote the larger public interest in the availability of important information would specify the public agencies to which the report will be submitted, including, for instance, the U.S. EAC, NIST, NASED, and the State's chief election officer.

Examination security: A forensic examination must be conducted under secure conditions. The specific expectations should be listed in the written contract. Frequently, the security precautions required for access to voting systems and ballots (such as the two-persons present at all times rule) should apply to the forensic team as well. Depending on the nature of the examination, the necessary security may require special secure environments to be created in which to do the work, with key control, video surveillance, guards, and so forth. The costs for these arrangements must be borne by whatever agency is in charge of the examination. Team members must also protect the intellectual property of the vendor, particularly any vendor-owned source code, both during and after the examination. Finally, the examiners must take steps to prevent any exploitable security vulnerabilities they may discover from becoming public knowledge.

Technical resources: The forensic team will request tools and resources as needed, and will need to receive them ***in a timely manner***. These requested resources are almost certain to include the source code because that is the set of commands for the computers. Normally, all parties (officials, courts, vendors, and others) should seek to expedite the review and supply the resources under their control. Any problems in providing those resources will impact the delivery date of the forensic report, and possibly damage its credibility. Contractually providing all parties with a mandatory timetable and prompt follow up procedures when delays occur may help keep the examination on track.

Role of vendors: The vendor's important role was discussed above in part VI.D but a few points will be reiterated here. The forensic contract or an addendum contract between the public agency and the vendor should specify the roles the vendor will play, including the timetable for vendor supply of specified resources, technical support, and permission for team access to the source code and build environment. It should record the decision regarding the sequencing of the vendor's receipt of and opportunity to respond to the forensic team report. The primary choices are for the vendor to receive a draft with an opportunity to respond pre-release, or to receive a copy post-public release. Another clause should detail how the vendor's response will be treated (e.g., a posted link accompanying the team's web-posted report). The contract should clarify the types of contact the team may have with the vendor, and specify the terms for the arm's-length relationship with the vendor, including the vendor having no role in the forensic team's assessments other than suggesting potential causes for the problem.

Vendor cooperation can greatly enhance the speed of the forensic review and lower its costs. Such cooperation can ultimately promote the vendor's opportunities to benefit from the examination. Vendors who quickly authorize source code review (under carefully constructed legal terms) and deliver the necessary materials can profit from learning whether there is a problematic point so that it can promptly be corrected for other jurisdictions/customers within the governing certification regime. Professional examiners will not violate the Digital Millennium Copyright Act to access and reviewing source code for a suspected error. Public authorities can (and, we believe, should) praise the vendor for speedy and complete cooperation in the forensics review.

To further promote this arm's-length relationship and avoidance of conflicts of interest, the vendor should not directly pay for the examination although, in some cases, depending on the State and forensic conclusions, it may be appropriate for government authorities to charge back to the vendor part or all of the expenses.

Costs: The cost of an examination can vary widely, and a budget must be agreed to as a part of the contract. The cost will vary depending on who conducts the examination. A forensic or security firm may charge more than academics who use the opportunity to involve graduate students, but a private firm may be able to sign a contract quickly. Costs, of course, go up with the complexity of the examination, the security arrangements required, and the travel necessitated. HAVA funds have been used for voting equipment reviews so this may be one source of financial support.

VIII. Conclusion

As we conclude this paper, the 2008 general election is just under one month away. In the presidential race—and in many other state, county, and local elections across this country—recent history counsels that some jurisdictions will experience some serious electoral complications. The job of the elections official has never, we think, been more important.

Because we respect the elections process and the people who practice and protect it, we have authored and made available this introductory overview of when and how to convene forensic reviews. It reflects our work in the real world of elections with dedicated election officials whom we count as friends and valued associates. We hope it proves useful as elections officials, candidates, vendors, observers, and citizens once again conduct the most fundamental exercise of democratic liberty.

ENDNOTE

7.1 The authors of this article expressly disclaim any intention to offer or suggest legal advice to any reader or official, and are only outlining the types of issues that will need to be resolved. Legal advice must come from licensed legal counsel engaged to offer it to their client. The materials assembled here by the authors should not be relied on as legal advice or passed on to others as such. Readers should consult with their own privately or publicly retained or authorized attorneys in making any legal decisions. (Thanks to our reviewers for suggestions on phrasing.)

Background on Authors

Matt Bishop Matt Bishop is a professor in the Department of Computer Science at the University of California at Davis, where he is a co-director of the Computer Security Laboratory. His research specializes in the analysis of computer system vulnerabilities. His interest in electronic voting systems began when California county election officials asked him about the security of their systems. He has participated in several scientific analyses of electronic voting systems, including the forensics analysis of the problematic 2006 contested Florida congressional district CD-13 race and the RABA 2004 review of Maryland's e-voting systems. He was a co-Principal Investigator for the California Top-to-Bottom Review (2007). Prof. Bishop has been a member of the Voting Systems Technology Assessment Advisory Board for the State of California, and works with his local Clerk-Recorder on election security in his county. Currently, his research group is examining the election process to guide the specification and analysis of e-voting systems. His textbook, *Computer Security: Art and Science*, is used in both undergraduate and graduate computer security classes at many universities.

Mark Graff is Chief Cyber Security Strategist of Lawrence Livermore National Laboratory. He has appeared as an expert witness on computer security before both Congress and the Presidential Commission on Infrastructure Survivability, and served as an expert witness on electronic voting machine software for the state of California. A former chairman of the international Forum of Incident Response and Security Teams (FIRST), Mr. Graff has lectured on risk analysis, the future of privacy, and other security-related topics before the American Academy for the Advancement of Science, the Federal Communications Commission, the Pentagon, and many other U.S. national security facilities and "think tanks." His most recent book, *Secure Coding: Principles and Practices* (co-authored with Ken van Wyk), is used at dozens of universities around the world to teach how to design and build secure software-based systems.

Candice Hoke is the founding Director of the *Center for Election Excellence* and a law professor at Cleveland State University with Election Law and Governance, and Regulatory Law specializations. She was a research Team Leader for the California Secretary of State's scientific study of voting systems (TTBR, 2007), and a member of the Cuyahoga Election Review Panel (2006) that examined the causes and suggested cures for major election failure. She served as Project Director of the Public Monitor of Cuyahoga Election Reform (2006-08). She is a member of the American Bar Association's Advisory Commission to the Standing Committee on Election Law (2007-). For the Public Monitor, Professor Hoke proposed and led via the Center for Election Integrity the first post-election audit in Ohio (Cuyahoga, November 2006). She has drafted federal and Ohio election reform legislation, and has testified to Congress on election auditing as a component for assuring public trust in the election system. She was a *Yale Law Journal* editor, a judicial clerk for the U.S. Court of Appeals for the First Circuit, a litigator, and a staff member of the North Carolina Governor's Office before becoming a law professor.

David Jefferson A computer scientist at the intersection of computing and public elections for over a decade, Dr. David Jefferson works on supercomputing applications for national security at Lawrence Livermore National Laboratory. He has worked with five California Secretaries of State and with numerous election officials in improving California elections. Most recently, Jefferson was appointed by Secretary of State Debra Bowen as chair of the Post-Election Audit Standards Working Group that worked parallel to the Top to Bottom Review study of California voting systems. He also served as the chair of the SOS's Technical Advisory Board (TAB) under Secretary

Kevin Shelley, and then as chair of its successor Board under Secretary Bruce McPherson. In 1999, he led the technical side of an SOS task force in its study and report on Internet voting. He subsequently served on the National Science Foundation-Internet Policy Institute panel on Internet voting, and testified to the National Commission on Federal Election Reform organized by presidents Carter and Ford. He has consulted with numerous agencies and States on the subject of voting security, including for the Federal Election Commission and the Department of Defense. He is also a co-author of the SERVE Security Report (servesecurityreport.org), which detailed the security vulnerabilities in the Defense Department's proposed Internet voting system in 2004.

Sean Peisert conducts research in computer security at the University of California, Davis. His work focuses on computer forensic analysis, intrusion detection, vulnerability analysis, security policy modeling, and electronic voting. His most recent research has involved developing a formal model of computer forensic logging and auditing, and he is now researching methods of applying the results to e-voting machines. Dr. Peisert gave the keynote address at the 2008 IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (IEEE/SADFE) and is the program committee co-chair of SADFE'09. Previously, he was a postdoctoral scholar and lecturer in the Computer Science and Engineering department at the University of California, San Diego (UCSD), was a computer security researcher at the San Diego Supercomputer Center (SDSC), and co-founded a software company. Dr. Peisert received his Ph.D., Masters and Bachelors degrees in Computer Science from UCSD. He is an I3P Fellow and is a Fellow of the San Diego Supercomputer Center.

Panel of Reviewers

This paper's co-authors appreciate and wish to thank the following diverse group of individuals whose commentary on draft versions (on very short notice) helped it to attain significant improvement. All errors and omissions are the authors' responsibility alone and no reviewer should be held accountable for our failures and time pressures.

Wayne Beckham, Chief Deputy, Riverside County (CA) Registrar of Voters

Charisse Castagnoli, Computer Security Professional and Adjunct Professor of Law, John Marshall Law School

Cindy Cohn, Legal Director, Electronic Frontier Foundation

David Dill, Professor, Stanford University, Department of Computer Science

John Eichhorst, Partner, Howard Rice Nemerovski Canady Falk & Rabkin, P.C.

Jeremy Epstein, Computer Security Consultant, CIGITAL

Sean Gallagher, Partner, Hogan & Hartson LLP, Denver, CO

Paul Hultin, Esq., Founding Partner, Wheeler Trigg Kennedy LLP, Denver, CO

Doug Jones, Associate Professor, University of Iowa, Department of Computer Science

David Klein, Elections Research and Operations Specialist, formerly office of Ohio Secretary of State

Michael Losavio, Lecturer, University of Louisville, Departments of Computer Engineering and Computer Science/Justice Administration

Lesley Mara, Deputy Secretary of State, Connecticut

Peter McLennon, Cook County (IL) Clerk's Office

Larry Norden, Counsel, Brennan Center for Justice of New York University

Freddie Oakley, Yolo County Clerk-Recorder

Marian K. Schneider, Attorney, Berwyn, PA

Fred Chris Smith, former Assistant U.S. Attorney and prolific author on forensic evidence

Alec Yasinsac, Dean and Professor, University of South Alabama, School of Computer and Information Sciences; Team Leader of the Florida CD-13 technical forensic examination.

Resources for Further Study

1. M. Bishop, "Overview of Red Team Reports," Office of the Secretary of State of California, 1500 11th St, Sacramento, CA 95814 (July 2007).

2. M. Bishop and D. Wagner, "Risks of E-Voting," *Communications of the ACM*, 50(11), p. 120 (Nov. 2007).

3. A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, "Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware," Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, FL 32306-4530 (Feb. 2007).

4. RABA Innovative Solution Cell, "Trusted Agent Report Diebold AccuVote-TS Voting System," RABA Technologies LLC, Columbia, MD 21045 (Jan. 2004).

5. D. Wagner, D. Jefferson, M. Bishop, C. Karlof, and N. Sastry, "Security Analysis of the Diebold AccuBasic Interpreter," Technical Report, Voting Systems Technology Assessment Advisory Board, Office of the Secretary of State of California, Sacramento, CA 95814 (Feb. 2006).

6. "Project EVEREST (Evaluation and Validation of Election-Related Equipment, Standards, and Testing) Risk Assessment Study of Ohio Voting Systems: Executive Report," Office of the Secretary of State of Ohio, Columbus, OH (Dec. 2007).

7. M. Clarkson, B. Hay, M. Inge, A, Shelat, D. Wagner, and A. Yasinsac, "Software Review and Security Analysis of Scytl Remote Voting Software," Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, FL 32306-4530 (Sep. 2008).

Appendix 1: Example of Nondisclosure Agreement in Voting Equipment Review

From the California Top-to-Bottom Review (2007), contract between the California Secretary of State and the University of California but terms largely negotiated by academic Principal Investigators found at http://www.sos.ca.gov/elections/voting_systems/ttbr/sos_uc_contract.pdf

Exhibit A, Section 11, page 10, relevant text:

> No confidential information, record or data identified as proprietary or confidential that is provided or accessed that directly pertains or exclusively relates to this voting system review shall be discussed, published, disclosed, transferred or otherwise communicated outside the scope of the voting system review. No confidential documents, files, papers, records, computer disks, or other tangible matters containing such proprietary or confidential data, files or records shall be removed from secured locations without express written permission of one of the Principal Investigators. These confidentiality restrictions shall apply only to material that is received from the State and identified in writing as confidential. The following information shall not be considered confidential information for the purposes of these restrictions: information that was already known to the receiving party, other than under an obligation of confidentiality, at the time of disclosure; or information that is now or hereafter becomes publicly known by other than a breach of the nondisclosure agreements associated with this project. These restrictions shall not be construed to prevent team members from conducting future research on voting systems, possibly including the ones examined in this review, after the completion of this project, so long as that research does not improperly use confidential information gained through this review. The Principal Investigator of each UC team shall be responsible for requiring all members of the UC team, and any other project participants, to execute acknowledgements that they have read, understood and agreed to abide by the terms and conditions of this Statement of Work. Such executed acknowledgement shall remain in effect for the duration of the project even in the event of resignation or termination of the UC team member or participant. Upon completion of the final report, all proprietary or confidential information, data, and documentation, original and copies, provided by the SOS to UC shall be returned promptly to the attention. . . Secretary of State . . ..

Appendix 2: Partial List of Voting Systems Studies

This appendix lists several studies of voting systems. The voting systems listed are taken from the reports; note that different reports may refer to the same system in slightly different ways. Further, generic equipment (such as generic memory cards and Ethernet cables and switches) is omitted, even when listed in the reports.

Each entry has the name by which the report is commonly referred. When projects have multiple reports, only the lead report or reports are listed. All reports are available on the listed web pages. Several reports, including some forensic reviews in an election context, are listed at the end but not in reverse chronological order or in the format of the balance, as they were received as the

paper was going to press.

2008: Op Bravo/Scytl

Report: M. Clarkson, B. Hay, M. Inge, A, Shelat, D. Wagner, and A. Yasinsac, "Software Review and Security Analysis of Scytl Remote Voting Software," Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, FL 32306-4530 (Sep. 2008).\

URL: http://doe.dos.state.fl.us/voting-systems/pdf/FinalReportSept19.pdf

Voting System:

- Pnyx.core ODBP 1.0 remote voting software

2007: Ohio EVEREST

Report: "Project EVEREST (Evaluation and Validation of Election-Related Equipment, Standards, and Testing) Risk Assessment Study of Ohio Voting Systems: Executive Report," Office of the Secretary of State of Ohio, Columbus, OH (Dec. 2007). Additional reports available from teams based on vendor assignment.

URL:
http://www.sos.state.oh.us/SOS/elections/voterInformation/equipment/VotingSystemReviewFindings.aspx

Voting Systems:

- Premier, consisting of:
  - GEMS software version 1.18.24
  - AccuVote-TSX version 4.6.4
  - AccuVote-OS 2000 Precinct Optical Scanner version 1.96.6
  - AccuVote-OS Central Optical Scanner version 2.0.12
  - Digi Seriel to Ethernet Gateway version PortServer II
  - VC Programmer ST100
  - Mobile Electronic Poll Worker Tablet System
  - Elections Media Processor System with Elections Media Drive Tower
  - Voter Card Encoder Spyrus PAR2
- ES&S, consisting of:
  - Unity Election Management Software version 3.0.1.1
  - Automark 87000
  - iVotronic DRE 90998-BI, 91057-BL, 93038-BL
  - Precinct Optical Scanner Model 100
  - Central Optical Scanner Model 650
- Hart Intercivic, consisting of:
  - BOSS, as provided by the Secretary of State
  - Tally, as provided by the Secretary of State
  - Rally, as provided by the Secretary of State
  - Servo, as provided by the Secretary of State
  - Trans, as provided by the Secretary of State

- Ballot on Demand, as provided by the Secretary of State
- eCM Manager, as provided by the Secretary of State
- eCM Token, as provided by the Secretary of State
- JBC
- eSlate 3000 DRE version 4.0.1.9
- eScan Optical Scanner version 1.1.6

2007: Florida Diebold Supplemental Report, SAIT Lab

Report: D. Gainey, M. Gerke, and A. Yasinsac, "Software Review and Security Analysis of the Diebold Voting Machine Software: Supplemental Report", Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, FL 32306-4530 (Aug. 2007).

URL: http://doe.dos.state.fl.us/voting-systems/pdf/dieboldRepriseRep.pdf

Voting Systems:
- Diebold Voting System Software version 1.96.8

2007: Florida Diebold Report, SAIT Lab

Report: R. Gardner, A. Yasinsac, M. Bishop, T. Kohno, Z. Hartley, J. Kerski, D. Gainey, R. Walega, E. Hollander, and M. Gerke, "Software Review and Security Analysis of the Diebold Voting Machine Software", Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, FL 32306-4530 (July 2007).

URL: http://doe.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf

Voting Systems:
- Diebold Optical Scan firmware version 1.96.8
- Diebold Touch Screen firmware version 4.6.5
- Diebold Touch Screen bootloader version 1.3.6
- Diebold GEMS software version 1.18.25

2007: California Top to Bottom Review, University of California

Reports: M. Bishop, "Overview of Red Team Reports," Office of the Secretary of State of California, 1500 11th St, Sacramento, CA 95814 (July 2007); D. Wagner, "Principal Investigator's Statement on Protection of Security-Sensitive Information," Office of the Secretary of State of California, 1500 11th St, Sacramento, CA 95814 (Aug. 2007); and additional reports by vendor assignment by teams focused on Source Code, Red Team, Documentation Reviews. An omnibus Accessibility report is available rather than vendor-specific individual reports.

URL: http://www.sos.ca.gov/elections/elections_vsr.htm

Voting Systems:
- Diebold GEMS 1.18.24/AccuVote, consisting of:
  - GEMS software version 1.18.24

  - AccuVote-TSX with AccuView Printer Module and Ballot Station firmware version 4.6.4
  - AccuVote-OS (Model D) with firmware version 1.96.6
  - AccuVote-OS Central Count with firmware version 2.0.12
  - AccuFeed
  - Vote Card Encoder version 1.3.2
  - Key Card Tool software version 4.6.1
  - VC Programmer software version 4.6.1
- Hart Intercivic System 6.2.1, consisting of:
  - Ballot Now software version 3.3.11
  - BOSS software version 4.3.13
  - Rally software version 2.3.7
  - Tally software version 4.3.10
  - SERVO version 4.2.10
  - JBC version 4.3.1
  - eSlate/DAU version 4.2.13
  - eScan version 1.3.14
  - VBO version 1.8.3
  - eCM Manager, version 1.1.7
- Sequoia WinEDS version 3.1.012/Edge/Insight/400-C, consisting of:
  - WinEDS version 3.1.012
  - AVC Edge Model I firmware version 5.0.24
  - AVC Edge Model II firmware version 5.0.24
  - VeriVote Printer
  - Optech 400-C/WinETP firmware version 1.12.4
  - Optech Insight APX K2.10, HPX K1.42
  - Optech Insight Plus APX K2.10, HPX K1.42
  - Card Activator version 5.0.21
  - HAAT Model 50 version 1.0.69L
  - Memory Pack Reader (MPR) firmware version 2.15

2007: Center for Election Integrity, Cleveland State University

Report: Thomas P. Ryan and Candice Hoke, Cleveland State University
GEMS Tabulation Database Design Issues in Relation to Voting Systems Certification Standards

URL: http://www.usenix.org/events/evt07/tech/full_papers/ryan/ryan_html/

Voting System: Diebold GEMS software

2007: Kentucky Attorney General

Report: J. Epstein, Security Consultant

URL: http://www.eac.gov/program-areas/research-resources-and-reports/copy_of_docs/state-local-voting-system-reports

2007: University of Connecticut VoTeR Report

Report: A, Kiayias, L. Michel, A. Russell, and A. Shvartsman, "Integrity Vulnerabilities in the Diebold TSX Voting Terminal," VoTeR Center, University of Connecticut, Storrs, CT 06269 (July 2007).

URL: http://voter.engr.uconn.edu/voter/Report-TSX_files/TSXVoting_Terminal_Report.pdf

Voting System:

- Diebold AccuVote-TSx firmware version 4.6.4, bootloader version BLR7-1.2.1, Windows CE Operating System version WCER-410.2.1
- Diebold GEMS server version 1.18

2006: University of California Hart Report

Report: E. Proebstel, S. Riddle, F. Hsu, J. Cummins, F. Oakley, T. Stanionis, and M. Bishop, "An Analysis of the Hart Intercivic DAU eSlate," *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop* (Aug. 2007).

URL: http://www.usenix.org/events/evt07/tech/full_papers/proebstel/proebstel.pdf

Voting System:

- Hart Intercivic eSlate version 6.1, consisting of:
    - eSlate firmware version 4.1.3
    - JBC firmware version 4.1.3
    - VBO firmware version 1.7.5

2007: Florida CD-13 (SAIT Report)

Report: A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, "Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware," Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, FL 32306-4530 (Feb. 2007).

URL: http://election.dos.state.fl.us/reports/pdf/FinalAudRepSAIT.pdf

Voting System:

- ES&S iVotronic firmware version8.0.1.2

2006: Diebold AccuBasic

Report: D. Wagner, D. Jefferson, M. Bishop, C. Karlof, and N. Sastry, "Security Analysis of the Diebold AccuBasic Interpreter," Technical Report, Voting Systems Technology Assessment Advisory Board, Office of the Secretary of State of California, Sacramento, CA 95814 (Feb. 2006).

URL:
http://www.sos.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf

Voting Systems:
- Diebold AccuVote-OS with firmware version 1.96.6
- Diebold AccuVote-TSx with firmware version 4.6.4

2004: RABA Report

Report: RABA Innovative Solution Cell, "Trusted Agent Report Diebold AccuVote-TS Voting System," RABA Technologies LLC, Columbia, MD 21045 (Jan. 2004).

URL: http://nob.cs.ucdavis.edu/bishop/notes/2004-RABA/2004-RABA.pdf

Voting Systems:
- Diebold AccuVote-TS Voting System
- Diebold GEMS server

2003: Compuware Report

Report: "Direct Recording Electronic (DRE) Technical Security Assessment Report," Compuware Corporation, Columbus, OH 43229 (Nov. 2003).

URL: http://www.sos.state.oh.us/sos/upload/everest/01-compuware112103.pdf

Voting Systems:
- Diebold Election Systems, consisting of:
  - AccuVote-TS R6 firmware version 4.3.15
  - GEMS server version 1.18.18
- ES&S, consisting of:
  - iVotronic version 7.4.5.0
  - Unity Election System software version 2.2
- Hart InterCivic, consisting of:
  - eSlate 3000 version 2.1
  - JBC version 1.16
  - BOSS Election Management Software version 2.9.04
  - TALLY software version 2.9.08
  - SERVO software version 1.0.2
- Sequoia Voting Systems, consisting of:
  - AVC Edge version 4.1.D
  - Card Activator version 4.2
  - WinEDS Election Management Software version 2.6

Additional Reviews (with thanks to Prof. Doug Jones of the University of Iowa; this information will be organized for the next edition of this paper)

A forensics examination report for central-count mark-sense tabulators in Maricopa County Arizona: http://www.cs.uiowa.edu/~jones/voting/ArizonaDist20.pdf

A report on pre-election testing in Miami Dade County, Florida, with sections on central-count mark-sense tabulators and touch-screen machines, as well as general remarks on test design.

http://www.cs.uiowa.edu/~jones/voting/miamitest.pdf

Auditing elections -- a discussion of how to do sanity checks on election results and pin down discrepancies. Forensic auditing clearly wants this, although I was more interested in on-the-fly self-auditing during the process.

http://www.cs.uiowa.edu/~jones/voting/cacm2004.shtml

Developing a Methodology for Observing Electronic Voting, a report from the Carter Center, includes Prof. Jones' talk on perspectives on electronic voting. This provides a framework for thinking about not only observing (the Carter Center's interest) but also forensic investigation. Forensic investigators will want the answers to essentially all the questions on the Carter Center's work sheets.

http://www.cartercenter.org/documents/elec_voting_oct11_07.pdf

(Republished in extended form in ***From Power Outages to Paper Trails,*** IFES).